THE UNIVERSITY OF CHICAGO.
Founded by JOHN D. ROCKEFELLER.

ASYMPTOTIC EVALUATION OF CERTAIN TOTIENT SUMS.

A DISSERTATION

SUBMITTED TO THE FACULTIES OF THE GRADUATE SCHOOLS OF ARTS, LITERATURE AND SCIENCE, IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY (DEPARTMENT OF MATHEMATICS).

By
DERRICK NORMAN LEHMER.

June, 1900.

THE UNIVERSITY OF CHICAGO.
Founded by JOHN D. ROCKEFELLER.

ASYMPTOTIC EVALUATION OF CERTAIN TOTIENT SUMS.

A DISSERTATION

SUBMITTED TO THE FACULTIES OF THE GRADUATE SCHOOLS OF ARTS, LITERATURE AND SCIENCE, IN CANDIDACY FOR THE DEGREE OF DOCTOR OF PHILOSOPHY (DEPARTMENT OF MATHEMATICS).

By
DERRICK NORMAN LEHMER.

June, 1900.

Digitized by the Internet Archive
in 2026

https://archive.org/details/IA41533910_0100

Asymptotic Evaluation of certain Totient Sums.

By Derrick Norman Lehmer.

Introduction.

This investigation is the outcome of an attempt to account for what seems to be a remarkable law first observed in particular cases in 1895. It may be stated as follows:

Consider any set s of k linear forms, $an + b_i$ $(i = 1 \ldots . k)$, all of which have the same modulus a, and where $[a, b_i] = 1$.* Consider, further, a function $\Theta_s(x)$ such that $\Theta_s(x) = 1$ or 0, according as each of the prime divisors of x belongs to one of the forms of the set s or not. If then $\nu(x)$ denotes the number of distinct primes in x, we have

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \text{constant.}$$

In the following we shall prove this law where s is the set of linear forms belonging to a binary quadratic form. We shall also determine the constant in this case.

In the investigation of this law, it seemed necessary to construct a more general theory of what Professor Sylvester has called the Totient Function—the function which denotes the number of integers not greater than a given number and prime to it. Euler, the first to discuss the function, denotes it by $\pi(x)$. Sylvester denotes it by $\tau(x)$. Most continental writers follow Gauss, and denote it by $\phi(x)$. We shall denote it by $\phi_1(x)$, as a special case of a more general function $\phi_m(x)$, which we have called the Multiple Totient of x of multiplicity m, or the m-fold totient of x.

* $[a, b]$ here, as always, denotes the greatest common divisor of a and b.

CHAPTER I.

MULTIPLE TOTIENTS.

The ordinary totient of an integer x being defined as the number of integers y such that

$$x \geqq y \geqq 1$$

and

$$[x, y] = 1,$$

we have as a generalization the following definition:

DEFINITION: *The m-fold totient of an integer x is the number of different sets of integers*

$$x_1 x_2 \ldots . x_m$$

which satisfy the conditions

$$x \geqq x_i \geqq 1, \qquad (i = 1 \ldots . m),$$

and

$$[x, x_1, x_2, \ldots . , x_m] = 1.$$

Two sets are considered different unless they contain the same integers arranged in the same order.

Let x be given in terms of its component primes

$$x = \prod_{i=1}^{r} p_i^a.$$

Disregard for the moment the second condition. The number of sets is then x^m, since each of the m elements x_i may run independently through the values 1, 2, ... x. Now, among these values there are $\frac{x}{p_i}$ multiples of p_i. There will then be $\left(\frac{x}{p_i}\right)^m$ sets where each element is a multiple of p_i. Similarly, there will be $\left(\frac{x}{\prod_{i=1}^{s} p_i}\right)^m$ sets where each element is a multiple of $\prod_{i=1}^{s} p_i$. The familiar principle of cross-classification* gives as the required number of sets, $x^m \prod_{i=1}^{r}\left(1 - \frac{1}{p_i^m}\right)$, which is the formula for the m-fold totient of x, for $x \neq 1$.

---

*See note on the principle of cross-classification at the end of this chapter.

For $x = 1$ we have the m-fold totient equal to unity. Denoting it by $\phi_m(x)$, we have the theorem:

THEOREM I. *For* $x = \prod_{i=1}^{r} p^{a_i} \neq 1$,

$$\phi_m(x) = x^m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^m}\right),$$

and

$$\phi_m(1) = 1.$$

The formula for $\phi^m(x)$ may be written in different forms easily obtainable from this. Thus:

$$\phi_m(x) = \prod_{i=1}^{r} p_i^{m(a_i-1)}(p_i^m - 1),$$

with again the understanding that $\phi_m(1) = 1$. A third important form is given in the theorem:

THEOREM II.

$$\phi_m(x) = x^m \sum_{(d)} \frac{\mu(d)}{d^m},$$

the sum extending over all d's which are divisors of x, *and* μ *being Mertens's Function* (*cf. Crelle's Journal, vol.* LXXVII, p. 289, 1874), *defined as follows:*

$$\mu(1) = 1,$$

and

$$\mu(x) = (-1)^{\lambda} \text{ or } 0,$$

according as each of the λ *distinct primes in* x *occurs to the first power or not.*

We shall see that for every theorem connected with the ordinary totient $\phi_1(x)$ there is a corresponding one in the theory of the function $\phi_m(x)$. The following theorem is evident:

THEOREM III. *If* x *and* y *are relative primes,*

$$\phi_m(x)\,\phi_m(y) = \phi_m(xy).$$

Also we can show the following

THEOREM IV.

$$\sum_{(d)} \phi_m(d) = x^m,$$

the sum extending over all d's which are divisors of x.

For we have, when $x > 1$,

$$\phi_m(x) = \prod_{i=1}^{r} (p_i^{m\alpha_i} - p_i^{m(\alpha_i - 1)});$$

and the sum in question may be written

$$\prod_{i=1}^{r} \sum_{k=0}^{c_i} \phi_m(p_i^k).$$

Now for $k = 0$, $\phi_m(p_i^k) = 1$. Otherwise, it is given by the formula above as

$$p_i^{mk} - p_i^{m(k-1)}.$$

The terms of the sum are then seen to cancel in pairs except the last one, which is $p_i^{\alpha_i m}$. The expression is then equal to $\prod_{i=1}^{r} p_i^{\alpha_i m} = x^m$. Hence the theorem.

The following theorem is of importance also:

THEOREM V. $\phi_m(x^n) = x^{m(n-1)} \phi_m(x)$,

We have

$$\phi_m(x^n) = x^{mn} \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^m}\right)$$

and

$$\phi_m(x) = x^m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i^m}\right).$$

By division the theorem follows.

We shall need to express $\phi_m(xy)$ in terms of $\phi_m(y)$. To this end we prove the fundamental theorem:

THEOREM VI.

$$\phi_m(xy) = \prod_{i=1}^{\tau} [p_i^{m\alpha_i} - p_i^{m(\alpha_i - 1)} \lambda(y, p_i)] \phi_m(y),$$

where $\lambda(y, p_i) = 0$ *or* 1, *according as* p_i *is or is not a divisor of* y.

Let $y = l \prod_{i=1}^{r} p_i^{\beta_i}$, where $[l, x] = 1$, and $\beta_i \geqq 0$.

We have

$$\phi_m(xy) = \prod_{i=1}^{r} [p_i^{m(\alpha_i + \beta_i - 1)} (p_i^m - 1)] \phi_m(l);$$

$$= \prod_{i=1}^{r} [p_i^{m(\beta - 1)} (p_i^m - 1)] \prod_{i=1}^{r} p_i^{m\alpha_i} \phi_m(l).$$

If, now, $\beta_i \neq 0$, the expression $p_i^{m(\beta_i-1)}(p_i^m-1)\phi_m(l)$ is equal to $\phi_m(p_i^{\beta_i}l)$. If, however, $\beta_i = 0$, this change cannot be made, but in this event p_i is not a factor of y. Thus the product of the $p_i^{\beta_i}$'s that do go over into the ϕ_m function is, when multiplied by l, precisely y itself. The factor left outside when $\beta_i = 0$ is $p_i^{m(\alpha_i-1)}(p_i^m-1)$. If $\beta_i \neq 0$, the factor is $p_i^{m\alpha_i}$, and the theorem is proved.

It follows from this theorem that if y runs through the values 1, 2, 3, ... , the coefficient of $\phi_m(y)$ on the right will be periodic of period $\prod_{i=1}^{r} p_i$. For if $y \equiv y' \left(\mathrm{mod} \prod_{i=1}^{r} p_i\right)$, then p_i divides y when, and only when it divides y' or

$$\lambda(y, p_i) = \lambda(y', p_i),$$

For example, in the case of the ordinary totient, $(m = 1)$, we have for $x = 18$:

$$\begin{aligned}
\phi_1(18.1) &= 6\,\phi_1(1),\\
\phi_1(18.2) &= 12\,\phi_1(2),\\
\phi_1(18.3) &= 9\,\phi_1(3),\\
\phi_1(18.4) &= 12\,\phi_1(4),\\
\phi_1(18.5) &= 6\,\phi_1(5),\\
\phi_1(18.6) &= 18\,\phi_1(6).
\end{aligned}$$

The coefficients now recur, the period being $2.3 = 6$.

We define now two functions by the following equations:

$$\Phi_m(x, n, k) = \sum_{i=1}^{\left[\frac{x}{k}\right]} \phi_m(i^n k^n),$$

and

$$\Omega_m(x, n, k) = \sum_{i=1}^{\left[\frac{x}{k}\right]} \frac{\phi_m(ik)}{(i^n k^n)^m},$$

where m, n and k are positive integers greater than zero, and x is positive but not necessarily integral. $\left[\frac{x}{k}\right]$ denotes here, as always, the greatest integer in $\frac{x}{k}$. In studying these functions we shall also need the function $S(x, k)$ defined by the equation

$$S(x, k) = \sum_{i=1}^{[x]} i^k.$$

We shall also need the well-known theorem,

$$\left[\frac{[x]}{k}\right] = \left[\frac{x}{k}\right].$$

THEOREM VII.

$$\sum_{j=1}^{[x]} j^{m(n-1)} \Phi_m\left(\frac{x}{j}, n, 1\right) = S(x, mn).$$

To show this theorem, we take the first difference of the function on the left with respect to $[x]$. This may be written

$$\sum_{j=1}^{[x]} j^{m(n-1)} \left\{\Phi_m\left(\frac{x}{j}, n, 1\right) - \Phi_m\left(\frac{x-1}{j}, n, 1\right)\right\}.$$

Now, if j does not divide $[x]$, the expression in the braces will vanish. If, on the other hand, j is a divisor of $[x]$, d say,—then the expression in braces becomes

$$\Phi_m\left(\frac{[x]^n}{d^n}\right).$$

But this, by Theorem V, is equal to

$$\frac{[x]^{m(n-1)}}{d^{m(n-1)}} \Phi_m\left(\frac{[x]}{d}\right).$$

The first difference in question may then be written:

$$\sum_{(d)} [x]^{m(n-1)} \Phi_m\left(\frac{[x]}{d}\right),$$

where the sum is extended over all d's which are divisors of $[x]$. If we put $dd' = [x]$, this becomes

$$\sum_{(d')} [x]^{m(n-1)} \Phi_m(d'),$$

where again the sum extends over all the divisors, d', of $[x]$. By Theorem IV this is $[x]^{mn}$. Since now $\Phi_m(1, n, 1) = 1^{mn}$, the theorem follows.

In precisely the same way we can prove

THEOREM VIII.

$$\sum_{j=1}^{[x]} \frac{1}{j^{mn}} \Omega_m\left(\frac{x}{j}, n, 1\right) = S(x, -m(n-1)).$$

Making use of the well-known recursion formula for Mertens's Function (cf. Bachmann, "Zahlentheorie," vol. II, p. 310), we easily derive from the formula of Theorem VII the following:

THEOREM IX.

$$\Phi_m(x, n, 1) = \sum_{i=1}^{[x]} \mu(i)\, i^{m(n-1)} S\left(\frac{x}{i}, mn\right).$$

This theorem is of cardinal importance for the sequel, as is also the corresponding theorem for the Ω function, which is proved in precisely the same way starting from Theorem VIII.

THEOREM X.

$$\Omega_m(x, n, 1) = \sum_{i=1}^{[x]} \frac{\mu(i)}{i^{mn}} S\left(\frac{x}{i}, -m(n-1)\right).$$

Similar formulæ for the general case where $k > 1$ do not appear to be obtainable, but we may find a general reduction formula by which we may reduce the general formulæ.

THEOREM XI. If $k = \prod_{i=1}^{r} p_i^{a_i}$, and $k' = \frac{k}{p_r^{a_r}}$, *then*

$$\Phi_m(x, n, k) = p_r^{m(a_r n-1)}(p_r - 1)\,\Phi_m\left(\frac{x}{p_r^{a_r}}, n, k'\right) + p_r^{m(a_r n-1)}\,\Phi_m\left(\frac{x}{p_r^{a_r}}, n, p_r k'\right).$$

To prove this formula, we observe that when i is prime to p_r, we have, by Theorem VI,

$$\phi_m(i^n k^n) = p_r^{m(a_r n-1)}(p_r - 1)\,\phi_m(i^n k'^n).$$

Assuming for the moment that i is prime to p_r for $i = 1, 2, \ldots, \left[\frac{x}{k}\right]$, we get on the left by summing

$$\sum_{i=1}^{\left[\frac{x}{k}\right]} \phi_m(i^n k^n) = \Phi_m(x, n, k),$$

by definition. On the right, we have

$$p_r^{m(a_r n-1)}(p_r - 1) \sum_{i=1}^{\left[\frac{x}{k}\right]} \phi_m(i^n k'^n).$$

Now, since

$$\left[\begin{matrix} x \\ k \end{matrix}\right] = \left[\frac{\left[\frac{x}{p_r^{a_r}}\right]}{k'}\right],$$

this last is by definition

$$p_r^{m(a_r n-1)}(p_r-1)\,\Phi_m\left(\frac{x}{p_r^{a_r}}, n, k'\right).$$

We must now correct for those terms where i is not prime to p_r; that is, for

$$i = p_r,\ 2p_r,\ 3p_r,\ \ldots\ ,\ \left[\frac{\left[\frac{x}{k}\right]}{p_r}\right]p_r.$$

For such terms we have, by Theorem VI.

$$\phi_m(i^n k^n) = p_r^{ma_r n}\,\phi_m(i^n k'^n).$$

But we have already taken such terms with a coefficient $p_r^{m(a_r n-1)}(p_r-1)$, so we have only to add the sum

$$p_r^{m(a_r n-1)} \sum_{(i)} \phi_m(i^n k'^n);$$

where the sum is extended over the values of i as given above, viz.:

$$i = p_r,\ 2p_r\ \ldots\ .\ \left[\frac{\left[\frac{x}{k}\right]}{p_r}\right]p_r.$$

We might write this sum,

$$p_r^{m(a_r n-1)} \sum_{(i)} \phi_m(i^n p_r^n k'^n),$$

where now i takes the values

$$i = 1,\ 2,\ 3,\ \ldots\ .\ \left[\frac{\left[\frac{x}{k}\right]}{p_r}\right].$$

that is,

$$i = 1,\ 2,\ 3,\ \ldots\ .\ \left[\frac{\left[\frac{x}{p_r^{a_r}}\right]}{p_r k'}\right].$$

But

$$p_r^{m(a_r n-1)} \sum_{i=1}^{\left[\frac{\left[\frac{x}{p_r^{a_r}}\right]}{p_r k'}\right]} \Phi_m (i^n . p_r^n k'^n)$$

is by definition

$$p_r^{m(a_r n-1)} \Phi_m \left(\frac{x}{p_r^a}, n, p_r k' \right),$$

and the theorem is proved.

By using the last theorem as a recursion formula, we obtain the theorem:

THEOREM XII. *If* $k = \prod_{i=1}^{r} p_i^{a_i}$, *and* $k' = \frac{k}{p_r^{a_r}}$, *then*

$$\Phi_m (x, n, k) = p_r^{m(a_r n-1)} (p_r - 1) \sum_{j=0}^{l} p_r^{m(n-1)j} \Phi_m \left(\frac{x}{p_r^{a_r+j}}, n, k' \right),$$

where l *is the first value of* j *for which* $\left[\frac{x}{p_r^{a_r+j}}\right] = 0$.

This then is a reduction formula, by means of which the general function $\Phi_m (x, n, k)$ may be expressed as a rational integral function of $\Phi_m (x, n, 1)$. Similar theorems may be obtained for the Ω function. Corresponding to Theorem XI, we have

THEOREM XIII. *If* $k = \prod_{i=1}^{r} p_i^{a_i}$, *and* $k' = \frac{k}{p_r^{a_r}}$, *then*

$$\Omega_m (x, n, k) = p_r^{-m(a_r \overline{n-1}+1)} (p_r - 1) \Omega_m \left(\frac{x}{p_r^{a_r}}, n, k' \right)$$

$$+ p_r^{-m(a_r \overline{n-1}+1)} \Omega_m \left(\frac{x}{p_r^{a_r}}, n, p_r k' \right).$$

Corresponding to Theorem XII, we have

THEOREM XIV. *If* $k = \prod_{i=1}^{r} p_i^{a_i}$, *and* $k' = \frac{k}{p_r^{a_r}}$, *then*

$$\Omega_m (x, n, k) = p_r^{-m(a_r \overline{n-1}+1)} (p_r - 1) \sum_{j=0}^{l} p_r^{-mnj} \Omega_m \left(\frac{x}{p_r^{a_r+j}}, n, k' \right),$$

where l *is the first value of* j *for which* $\left[\frac{x}{p_r^{a_r+j}}\right] = 0$.

It is remarkable that the theorems for the function Ω may be obtained from those of the function Φ by changing n into $-(n-1)$, as if, indeed,

$$\Omega_m(x, n, k) = \Phi_m(x, -\overline{n-1}, k),$$

or as if the formula of Theorem V held for negative values of n, and

$$\frac{\phi_m(x)}{x^{nm}} = x^{-nm}\phi_m(x) = \phi_m(x^{-n+1}).$$

If, in fact, we take as a definition of $\phi_m(x^{-n})$,

$$\phi_m(x^{-n}) = \frac{\phi_m(x)}{x^{m(n-1)}},$$

the functions Ω and Φ are identical.

The special case of Theorem VII where $m = n = k = 1$ was discovered by Sylvester (Philosophical Magazine, 1883, p. 251).

NOTE.—The principle of cross-classification referred to on page 4 of this chapter, may be stated as follows (cf. H. J. S. Smith Works, vol. 1, p. 36):

Suppose, in a collection of N individuals, there are n different classes which are not mutually exclusive. Suppose there be given the number of individuals belonging in each class. It is required to determine the number of individuals which belong to *none* of the n classes.

With the notation $N_\lambda(a_{i_1}, a_{i_2}, \ldots a_{i_\lambda})$ to denote the number of individuals belonging at the same time to each of the λ classes $a_{i_1} \ldots a_{i_\lambda}$, the answer to the problem may be written

$$\sum_{\lambda=0}^{n} \sum_{i=1}^{\frac{n!}{\lambda!(n-\lambda)!}} (-1)^\lambda N_\lambda(a_{i_1}, a_{i_2}, \ldots a_{i_\lambda}),$$

where $N_0 = 0$.

For, consider the effect of the above on an individual that occurs in ν classes. For $\lambda = 1$ it is subtracted ν times. For $\lambda = 2$ it is added $\frac{\nu(\nu-1)}{2!}$ times, and in general for $\lambda = r$, it is added or subtracted

$$\frac{\nu(\nu-1)(\nu-2)\ldots(\nu-\overline{r-1})}{r!}$$

times, according as r is even or odd. The resulting effect for $\lambda = 1, 2, 3, \ldots . \nu$ is expressed by the sum

$$\nu - \frac{\nu(\nu-1)}{2!} + \frac{\nu(\nu-1)(\nu-2)}{3!} - \ldots . \pm \frac{\nu(\nu-1) \ldots . (\nu-\overline{r-1})}{r!} \pm \ldots ,$$

which is $-1+(1-1)^\nu$. If $\nu = 0$, the individual belongs to none of the subclasses and remains undisturbed by the above process. If $\nu \neq 0$, the individual has been rejected once as was desired.

In certain cases of frequent occurrence in the Theory of Numbers, the above sum may be greatly simplified. If the number of individuals belonging simultaneously to the classes $a_{i_1}, a_{i_2}, \ldots . a_{i_l}$ be given by $N.\phi(a_{i_1} \ldots . a_{i_l})$, where ϕ is such a function that

$$\phi(x)\,\phi(y) = \phi(xy),$$

then the above sum may be put into the product form:

$$N\prod_{i=1}^{n}(1-\phi(a_i)).$$

CHAPTER II.

Approximative Formulæ for Multiple Totients.

We propose in this chapter to develop certain formulæ of approximation for the functions Φ and Ω. The results are, in fact, generalizations of the well-known formula for the totient function (Dirichlet, Werke, vol. II, p. 60; Mertens, Crelle's Journal, vol. LXXVII, p. 289, 1874).

It will be necessary, first of all, to obtain a formula for the sum $S(x, n)$ defined on page 8. Such a formula has already been obtained for positive integral values of x and n by Nöel in Quetelet's Correspondance Mathématique, vol. 1, p. 124, where use is made of it to prove certain theorems in geometry and mechanics. For our purposes, however, it will be necessary to remove the above restrictions on x and n except that x is supposed positive.

THEOREM 1. *For all positive values of x and n,*

$$S(x, n) = \frac{x^{n+1}}{n+1} + \Delta_{S(x, n)},$$

where $$|\Delta_{S(x,\,n)}| \leqq x^n.$$

We assume first that x is an integer, and show that in this case

$$0 \leqq \Delta_{S(x,\,n)} \leqq x^n.$$

We have

$$\Delta_{S(\overline{x,\,+1},\,n)} = \Delta_{S(x,\,n)} + (x+1)^n + \frac{x^{n+1}}{n+1} - \frac{(x+1)^{n+1}}{n+1}.$$

If, now, we assume $\Delta_{S(x,\,n)} \geqq 0$, then

$$\Delta_{S(\overline{x+1},\,n)} \geqq (x+1)^n + \frac{x^{n+1}}{x+1} - \frac{(x+1)^{n+1}}{n+1}.$$

But by Taylor's theorem,

$$\frac{(x+1)^{n+1}}{n+1} = \frac{x^{n+1}}{n+1} + (x+\theta)^n,$$

where $0 \leqq \theta \leqq 1$. We thus obtain

$$\begin{aligned}\Delta_{S(\overline{x+1},\,n)} &\geqq (x+1)^n - (x+\theta)^n,\\ &\geqq 0.\end{aligned}$$

If, therefore, $\Delta_{S(x,\,n)} \geqq 0$, we will also have $\Delta_{S(\overline{x+1},\,n)} \geqq 0$. But $\Delta_{S(1,\,n)} = \frac{n}{n+1} > 0$, for $n > 0$. Therefore, in general, $\Delta_{S(x,\,n)}$ is positive. Again if we assume

$$\Delta_{S(x,\,n)} \leqq x^n,$$

we have

$$\Delta_{S(\overline{x+1},\,n)} \leqq x^n + (x+1)^n - \frac{(x+1)^{n+1}}{n+1} + \frac{x^{n+1}}{n+1}.$$

But again, by Taylor's theorem,

$$\frac{(x+1)^{n+1}}{n+1} = x^{n+1} + x^n + n(x+\theta)^{n-1},$$

where $0 \leqq \theta \leqq 1$. We thus obtain

$$\Delta_{S(\overline{x+1},\,n)} \leqq (x+1)^n - n(x+\theta)^{n-1},$$

which, being positive, is less than $(x+1)^n$. Again, since $\Delta_{S(1,\,n)} = \frac{n}{n+1} < 1^n$, the theorem as stated is true for all integer values of x.

Let, now, x be any positive number. Then we have

$$S(x, n) = \frac{[x]^{n+1}}{n+1} + \Delta_{S(x, n)},$$

as above. Put now $[x] = x - \sigma_x$, where $0 \leqq \sigma_x < 1$, and we have, by Taylor's theorem,

$$\frac{[x]^{n+1}}{n+1} = \frac{(x-\sigma_x)^{n+1}}{n+1} = \frac{x^{n+1}}{n+1} - \sigma_x (x - \theta\sigma_x)^n,$$

where $0 \leqq \theta \leqq 1$. We have, therefore,

$$S(x, n) = \frac{x^{n+1}}{n+1} + \Delta'_{S(x, n)},$$

where $$\Delta'_{S(x, n)} = \Delta_{S(x, n)} - \sigma_x (x - \theta\sigma_x)^n.$$

Now, both terms on the right are essentially positive, and their difference is less than the greater of them. The greatest value of $\sigma_x (x - \theta\sigma_x)^n$ is obtained by putting $\sigma_x = 1$, $\theta = 0$, which gives x^n. The theorem follows.

THEOREM II. *For* $x \geqq 1$,

$$S(x, -1) = \log x + \Delta_{S(x, -1)},$$

where $$|\Delta_{S(x, -1)}| \leqq 4.$$

We have a well-known formula for $S(x, -1)$, (cf. Boole, "Finite Differences," p. 93), when x is integral, namely:

$$S(x, -1) = \log x + \Delta_{S(x, -1)},$$

where

$$\Delta_{S(x, -1)} = \varepsilon + \frac{1}{2x} + \sum_{i=1}^{\infty} (-1)^i \frac{B_{2i-1}}{(2i)!} \frac{1}{(2i)x^{2i}}.$$

(ε denotes Euler's constant .577215 ...., and the B's are Bernaulli's numbers.)

It is seen at once that

$$|\Delta_{S(x, -1)}| \leqq \varepsilon + \tfrac{1}{2} + \sum_{i=1}^{\infty} \frac{B_{2i-1}}{(2i)!} \frac{1}{2i}.$$

But we also have (Boole, "Finite Differences," p. 109),

$$\frac{B_{2i-1}}{(2i)!} = \frac{2}{(2\pi)^{2i}} \sum_{j=1}^{\infty} \frac{1}{j^{2i}} \leq \frac{2}{(2\pi)^{2i}} \cdot \frac{\pi^2}{6} .$$

Also, since $(2\pi)^{2i} > \frac{\pi^2}{6} i$, we have

$$\frac{B_{2i-1}}{(2i)!} < \frac{2}{i} ;$$

so that

$$|\Delta_{S(x,-1)}| \leq \varepsilon + \tfrac{1}{2} + \sum_{i=1}^{\infty} \frac{1}{i^2} ,$$
$$< 3 .$$

In case x is not an integer, we have as above,

$$S(x, -1) = \log [x] + \Delta_{S(x,-1)} ,$$

and putting $[x] = x - \sigma_x$, where $0 \leq \sigma_x < 1$,

$$S(x, -1) = \log x - \log \left(1 - \frac{\sigma_x}{x}\right) + \Delta_{S(x,-1)} .$$

We wish to examine the absolute value of

$$\log \left(1 - \frac{\sigma_x}{x}\right) , \text{ or of } \log \left(1 - \frac{\sigma_x}{[x] + \sigma_x}\right) .$$

Now, for $[x] \geq 1$, we have

$$\left| \log \left(1 - \frac{\sigma_x}{[x] + \sigma_x}\right) \right| \leq \left| \log \left(1 - \frac{\sigma_x}{1 + \sigma_x}\right) \right| ,$$

and since $\sigma_x < 1$,

$$\left| \log \left(1 - \frac{\sigma_x}{[x] + \sigma_x}\right) \right| \leq \log \tfrac{1}{2} < 1 ,$$

and the theorem follows.

THEOREM III. *For $x \geq 1$, and $n > 1$,*

$$S(x, -1) = D_{(n)} + \Delta_{S(x,-n)} ,$$

where

$$D_{(n)} = \sum_{j=1}^{\infty} \frac{1}{j^n} , \text{ and } |\Delta_{S(x,-n)}| \leq \frac{1}{[x]} .$$

We have

$$\Delta_{S(x,-n)} = -\sum_{j=[x]+1}^{\infty} \frac{1}{j^n} ,$$

so

$$|\Delta_{S(x,-n)}| \leqq \sum_{j=[x]+1}^{\infty} \frac{1}{j(j-1)} \leqq \frac{1}{[x]}.$$

We can now find an approximate formula for our function

$$\Phi_m(x, n, 1).$$

THEOREM IV.

$$\Phi_m(x, n, 1) = \frac{x^{mn+1}}{mn+1} \frac{1}{D_{(m+1)}} + \Delta\Phi_m(x, n, 1),$$

where

$$D_{(m+1)} = \sum_{j=1}^{\infty} \frac{1}{j^{n+1}} \text{ and } |\Delta\Phi_m(x, n, 1)| \leqq Ax^{mn} \log x,$$

A being finite and independent of x, m *and* n.

We start from Theorem X of the preceding chapter,

$$\Phi_m(x, n, 1) = \sum_{i=1}^{[x]} \mu(i) i^{m(n-1)} S\left(\frac{x}{i}, mn\right).$$

Writing in our formula for $S\left(\frac{x}{i}, mn\right)$, this becomes equal to $M+N$, where

$$M = \sum_{i=1}^{[x]} \frac{\mu(i) x^{mn+1}}{(mn+1) i^{m+1}}$$

and

$$N = \sum_{i=1}^{[x]} \mu(i) i^{m(n-1)} \Delta_S\left(\frac{x}{i}, mn\right).$$

since now

$$\left|\Delta_S\left(\frac{x}{i}, mn\right)\right| \leqq \frac{x^{mn}}{i^{mn}},$$

we have, putting $\mu(i) = 1$,

$$|N| \leqq x^{mn} \sum_{i=1}^{[x]} \frac{1}{i^m}.$$

Since $m \geqq 1$,

$$|N| \leqq x^{mn} \sum_{i=1}^{[x]} \frac{1}{i},$$
$$\leqq A_1 x^{mn} \log x,$$

where A_1 is finite and independent of x, m and n.

We break up M into two parts:

$$M = P + Q,$$

where

$$P = \frac{x^{mn+1}}{mn+1} \sum_{i=1}^{\infty} \frac{\mu(i)}{i^{m+1}},$$

$$= \frac{x^{mn+1}}{mn+1} \frac{1}{D_{(m+1)}},$$

and

$$Q = \frac{-x^{mn+1}}{mn+1} \sum_{i=[x]+1}^{\infty} \frac{\mu(i)}{i^{m+1}}.$$

Now

$$|Q| \leqq \frac{x^{mn+1}}{mn+1} \sum_{i=[x]+1}^{\infty} \frac{1}{i^2},$$

$$< \frac{x^{mn+1}}{mn+1} \sum_{i=[x]+1}^{\infty} \frac{1}{i(i-1)},$$

$$\leqq \frac{x^{mn+1}}{mn+1} \frac{1}{[x]},$$

$$\leqq A_2 x^{mn},$$

$$\leqq A_2 x^{mn} \log x,$$

where A_2 is finite and independent of x, m and n. The theorem follows.

THEOREM V. *For any prime $p > 1$,*

$$\Phi_m(x, n, p^a) = \frac{x^{mn+1}}{mn+1} \frac{p-1}{p^{a-1}(p^{m+1}-1)} \frac{1}{D_{(m+1)}} + \Delta\Phi_m(x, n, p^a),$$

where $D_{(m+1)}$ is defined as in the preceding theorem, and

$$|\Delta\Phi_m(x, n, p^a)| \leqq A x^{mn} \log x,$$

A being finite and independent of x, m and n.

By Theorem XII of the preceding chapter we have

$$\Phi_m(x, n, p^a) = p^{m(an-1)}(p-1) \sum_{j=0}^{l} p^{m(n-1)j} \Phi_m\left(\frac{x}{p^{a+j}}, n, 1\right),$$

where l is the first value of j for which $\left[\frac{x}{p^{a+j}}\right] = 0$. Put in this expression the value of $\Phi_m(x, n, 1)$ obtained in the preceding theorem. We may write the result equal to $M + N$, where

$$M = \frac{(p-1)x^{mn+1} D_{(m+1)}}{(mn+1)p^{a+m}} \sum_{j=0}^{l} \frac{1}{p^{(m+1)}};$$

and

$$N = p^{m(an-1)}(p-1)\sum_{j=0}^{l} p^{m(n-1)j}\,\Delta\Phi_m\left(\frac{x}{p^{a+j}}, n, 1\right).$$

We have then

$$|N| \leqq A_1 \frac{(p-1)}{p^m} x^{mn}\log x \sum_{j=0}^{l}\frac{1}{p^{jm}},$$
$$\leqq A_2 x^{mn}\log x,$$

where A_2 is finite and independent of x, m and n. Also we may write

$$M = P + Q,$$

where

$$P = \frac{(p-1)}{p^{a+m}}\,\frac{x^{mn+1}}{mn+1}\,\frac{1}{D_{(m+1)}}\sum_{j=0}^{\infty}\frac{1}{p^{(m+1)j}}.$$

and

$$Q = -\frac{p-1}{p^{a+m}}\,\frac{x^{mn+1}}{mn+1}\,\frac{1}{D_{(m+1)}}\sum_{j=l+1}^{\infty}\frac{1}{p^{(m+1)j}}.$$

Now

$$\sum_{j=l+1}^{\infty}\frac{1}{p^{(m+1)j}} = \frac{1}{p^{(m+1)l}}\cdot\frac{1}{p^{m+1}-1},$$

and from our definition of l,

$$p^{a+l+1} > x.$$

Since p occurs to a higher power than this in the denominator on the right in the equation for Q, we may write

$$|Q| \leqq A_3 x^{mn} \leqq A_3 x^{mn}\log x,$$

where A_3 is finite and independent of x, m and n.

Finally, since

$$P = \frac{x^{mn+1}}{mn+1}\,\frac{1}{D_{(m+1)}}\,\frac{p-1}{p^{a-1}(p^{m+1}-1)},$$

the theorem is proved.

We will now derive a formula of approximation for $\Phi_m(x, n, k)$. For shortness of expression, we define a function $P(m, k)$ by the equation

$$P_{(m,k)} = \prod_{i=1}^{r}\frac{p_i-1}{p_i^{a_i-1}(p_i^{m+1}-1)},$$

where $k = \prod_{i=1}^{r} p_i^{a_i}$, and where also we understand

$$P_{(m,1)} = 1.$$

We denote also, as in the preceding theorems, by $D_{(k)}$ the sum $\sum_{i=1}^{\infty} \frac{1}{i^k}$.

We prove now the general theorem:

THEOREM VI.

$$\Phi_m(x, n, k) = \frac{x^{mn+1}}{mn+1} \frac{P_{(m,k)}}{D_{(m+1)}} + \Delta\Phi_m(x, n, k),$$

where

$$|\Delta\Phi_m(x, n, k)| \leq Ax^{mn} \log x,$$

A being finite and independent of x, m *and* n.

Suppose that the theorem holds for $\Phi_m(x, n, k')$, where $k' = \frac{k}{p_r^{\alpha_r}}$, k being equal to $\prod_{i=1}^{r} p_i^{\alpha_i}$.

We have, by Theorem XII of the preceding chapter,

$$\Phi_m(x, n, k) = p_r^{m(\alpha_r n-1)}(p_r - 1) \sum_{j=0}^{l} p_r^{m(n-1)j} \Phi_m\left(\frac{x}{p_r^{\alpha_r+j}}, n, k'\right),$$

where l is the first value of j for which $\left[\frac{x}{p_r^{\alpha_r+j}}\right] = 0$. By the hypothesis we may write this equal to $M + N$, where

$$M = \frac{p_r - 1}{p_r^{m+\alpha_r}} \frac{x^{mn+1}}{mn+1} \frac{P_{(m,k')}}{D_{(m+1)}} \sum_{j=0}^{l} \frac{1}{p_r^{(m+1)j}},$$

and

$$N = p_r^{m(\alpha_r n-1)}(p_r - 1) \sum_{j=0}^{l} p_r^{m(n-1)j} \Delta\Phi\left(\frac{x}{p_r^{\alpha_r+j}}, n, k'\right).$$

We may, then, proceed exactly as in the preceding theorem, and the result shows that if the theorem is true for k' it is true for k. But in the preceding theorem we have proved it for $k = p^\alpha$. It is, therefore, true in general.

For the particular case of the ordinary totient, we have $m = n = k = 1$, and $P(mk) = 1$, while $D_{(2)} = \frac{\pi^2}{6}$. Our formula gives, therefore,

$$\frac{3}{\pi^2} x^2 + \Delta,$$

where $|\Delta| \leq Ax \log x$; a well-known result (Dirichlet, Werke, vol. II, p. 60; Mertens, Crelle's Journal, vol. LXXVII, p. 289, 1874).

The above results may be looked upon as theorems in connection with the function $\Omega_m(x, n, k)$, where n is negative or zero. The case $n = 1$ is important for the sequel, and a treatment precisely similar to the one used above will give

THEOREM VII.

$$\Omega_m(x, 1, k) = x\frac{P_{(m,k)}}{D_{(m+1)}} + \Delta_{\Omega m}(x, 1, k),$$

where

$$|\Delta_{\Omega m}(x, 1, k)| \leqq A \log x,$$

A being finite and independent of x, m and n.

This is seen to be the same as would be obtained by the formula for $\Phi_m(x, 0, k)$.

The case $\Omega_1(x, 2, k)$ must be treated separately, since in that case $S\left(\frac{x}{i}, -m(n-1)\right)$ becomes $S\left(\frac{x}{i}, -1\right)$, and the formula of Theorem II must be employed. We start with Theorem X of the preceding chapter and write

$$\Omega_1(x, 2, 1) = \sum_{i=1}^{[x]} \frac{\mu(i)}{i^2} S\left(\frac{x}{i}, -1\right);$$

which gives $\Omega_1(x, 2, 1) = M + N$, where

$$M = \sum_{j=1}^{[x]} \frac{\mu(j)}{j^2} \log\left(\frac{x}{j}\right),$$

and

$$N = A\sum_{j=1}^{[x]} \frac{\mu(j)}{j^2}.$$

Therefore,

$$|N| \leqq A\frac{6}{\pi^2} \leqq A_1,$$

A_1 being finite and independent of x.

We also write

$$M = P + Q,$$

where

$$P = \sum_{j=1}^{[x]} \frac{\mu(j)}{j^2} \log x,$$

and

$$|Q| \leqq \sum_{j=1}^{[x]} \frac{\log j}{j^2}.$$

Now $\log j < j^{\frac{1}{2}}$, so

$$|Q| \leqq \sum_{j=1}^{\infty} \frac{1}{j^{1+\frac{1}{2}}}.$$

which is a finite series (cf. Dirichlet-Dedekind, "Zahlentheorie," p. 304).

Finally, we put $P = R + S$, where

$$R = \log x \sum_{j=1}^{\infty} \frac{\mu(j)}{j^2} = \frac{\log x}{D_{(2)}},$$

and

$$|S| \leqq \log x \sum_{j=[x]+1}^{\infty} \frac{1}{j(j-1)} \leqq \frac{\log x}{[x]} < 1.$$

Collecting results, we have

$$\Omega_1(x, 2, 1) = \frac{\log x}{D_2} + \Delta_{\Omega_1(x, 2, 1)},$$

where

$$|\Delta_{\Omega_1(x, 2, 1)}| \leqq A,$$

A being finite and independent of x. From this point the discussion runs parallel to the discussion of Theorems V and VI. We obtain thus the theorem:

THEOREM VIII.

$$\Omega_1(x, 2, k) = \log x \frac{P_{(1, k)}}{D_{(2)}} + \Delta_{\Omega_1(x, 2, k)},$$

where $|\Delta_{\Omega_1(x, 2, k)}| \leqq A$, *where* A *is finite and independent of* x.

The remaining values of μ are now readily disposed of. We can prove the theorem:

THEOREM IX. *For* $n > 2$, $x \geqq 1$,

$$\Omega_m(x, n, k) = \frac{D_{(m, \overline{n-1})}}{D_{(mn)}} + \Delta_{\Omega_m(x, n, k)},$$

where $|\Delta\Omega_m(x, n, k)| \leqq \frac{A}{[x]}$, *where* A *is finite and independent of* x.

We start with Theorem X of the previous chapter and write

$$\Omega_m(x, n, 1) = \sum_{j=1}^{[x]} \frac{\mu(j)}{j^{mn}} S\left(\frac{x}{j}, -m(n-1)\right),$$

and, by Theorem III of this chapter, we write this equal to $M + N$, where

$$M = D_{(m, \overline{n-1})} \sum_{j=1}^{[x]} \frac{\mu(j)}{j^{mn}},$$

and

$$N=\sum_{j=1}^{[x]} \frac{\mu(j)}{j^{mn}} \Delta \left(\frac{x}{j} - m(n-1)\right),$$

and by that same theorem,

$$|N| \leq \sum_{j=1}^{[x]} \frac{1}{j^{mn}} \div \left[\frac{x}{j}\right].$$

This we may write

$$|N| \leq \sum_{j=1}^{[x]} \frac{1}{j^2\left[\frac{x}{j}\right]}, \leq \left[\frac{1}{x}\right]^2 + \sum_{j=1}^{[x]-1} \frac{1}{j^2\left(\frac{x}{j}-1\right)}.$$

Now the expression $j^2\left(\frac{x}{j}-1\right)$ is a minimum when $j=\frac{x}{2}$. Giving it this value

$$|N| \leq \frac{1}{[x^2]} + \frac{[x]-1}{\frac{x^2}{4}}$$

$$< \frac{A_1}{[x]},$$

A_1 being independent of x, m and n.

Also, $M = P + Q$, where

$$P = D_{(m.\overline{n-1})} \sum_{j=1}^{\infty} \frac{\mu(j)}{j^{mn}},$$

$$= \frac{D_{(m.\overline{n-1})}}{D_{(mn)}};$$

and

$$|Q| \leq D_{(m.\overline{n-1})} \sum_{j=[x]+1}^{\infty} \frac{1}{j^{mn}}$$

$$\leq \frac{A_2}{[x]},$$

where A_2 is again finite and independent of x, m and n. The theorem is thus proved for $k=1$. The proof then proceeds as before.

CHAPTER III.

TOTIENT POINTS.

We define a totient point in space of m dimensions, as a point whose m coordinates are integers having unity for their greatest common divisor. Not

to restrict ourselves to positive or non-zero values of the coordinates, we define the greatest common divisor of any set of positive or negative integers, as the greatest common divisor of their absolute values, while the greatest common divisor of any number and zero is the number itself.

The existence of any one totient point with m coordinates involves the existence of $m!$ other totient points, obtained by permuting the coordinates of the point in all possible ways. These points may or may not all be distinct. This is a special case under the more general theorem which follows:

THEOREM I. *The effect of a linear homogeneous substitution with positive or negative integer coefficients and determinant positive or negative unity, is to transform totient points into totient points.*

From the equations of transformation it is manifest that any common divisor of the old coordinates must appear in the new. Solving for the old coordinates in terms of the new, we get again integer coefficients; and again, any common divisor of the new coordinates must appear also in the old. The theorem follows.

We define now an i-compartment of space of m dimensions, as the locus of points which are such that the i^{th} coordinate, x_i, of each is a fixed positive or negative integer, not zero, and if x_j is any other of the $m-1$ coordinates, $\left[\frac{x_j}{x_i}\right]$ is a definite fixed positive or negative integer (or zero).

Any given point lies in m different compartments, since the compartment may be taken with respect to any one of the m coordinates. We obtain an infinitude of compartments for each coordinate x_i by choosing different values of $\left[\frac{x_j}{x_i}\right]$.

THEOREM II. *There exists a one-to-one correspondence between the totient points of any two compartments, obtained by choosing different values of* $\left[\frac{x_j}{x_i}\right]$, *both compartments being taken with respect to the same coordinate* x_i.

By addition of suitable multiples of x_i to the remaining coordinates of a totient point in one compartment, we derive a totient point in the other. But we derive only one. For if any coordinate x_j go by this means to two coordinates x_j' and x_j'', we may write

$$x_j + \lambda_1 x_i = x_j',$$
$$x_j + \lambda_2 x_i = x_j'',$$

whence

$$\left[\frac{x_j}{x_i} + \lambda_1\right] = \left[\frac{x_j'}{x_i}\right],$$

and

$$\left[\frac{x_j}{x_i} + \lambda_2\right] = \left[\frac{x_j''}{x_i}\right].$$

But if x_j' and x_j'' belong to points in the same compartment,

$$\left[\frac{x_j'}{x_i}\right] = \left[\frac{x_i''}{x_i}\right],$$

and it follows easily that $\lambda_1 = \lambda_2$, and that the coordinates are the same.

THEOREM III. *The number of totient points in any compartment with respect to the coordinate x_i is $\phi_{m-1}(x_i)$.*

It will be remembered $\phi_{m-1}(x_i)$ indicates the number of sets

$$x_i, x_1, x_2, \ldots, x_{i-1}, x_{i+1} \ldots x_m,$$

where $x_i \geqq x_j \geqq 1$, for $j = 1, 2, \ldots m$, and $j \neq i$, and where also

$$[x_i, x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots x_m] = 1.$$

If, then, whenever any coordinate x_j is equal to x_i, we subtract x_i, thus reducing that coordinate to zero, we get a set satisfying the conditions

$$x_i > x_j \geqq 0, \qquad j = 1, 2, \ldots m \text{ and } j \neq i,$$

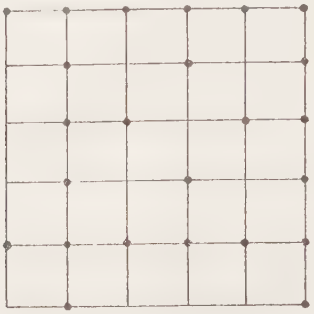
and also still

$$[x_i, x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_m] = 1.$$

We have, then, exactly $\phi_{m-1}(x_i)$ totient points where the coordinate x_i is the same in each, and where $\left[\frac{x_j}{x_i}\right] = 0$. All these points have positive or zero coordinates. They all lie in the same compartment, which, for convenience, we may call the zero compartment. Since the number is the same for each compartment, the theorem follows.

Example I. Take $m = 2$, $x_i = 6$. Then $\phi_{m-1}(x_i) = 2$. The compartments lie on the line $x = 6$. In the zero compartment are the points (6, 1) and (6, 5).

Example II. Take $m = 3$, $x_i = 6$. Then $\phi_{m-1}(x_i) = 24$. The compartments lie in the plane $x = 6$. In the zero compartment the points are arranged as in the figure:

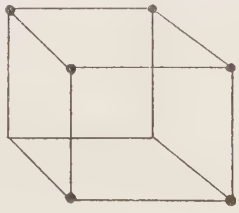


The points in the other compartments are arranged in precisely the same symmetrical way. One obtains the points in another compartment by adding multiples of six to the coordinates y and z of the points in the zero compartment.

Example III. Take $m = 4$, $x_i = 2$ Then $\phi_{m-1}(x_i) = 7$. The compartments are cubes. The zero compartment contains the seven points:

$$(1, 1, 1), (0, 1, 1), (1, 0, 1), (1, 1, 0), (0, 0, 1), (0, 1, 0), (1, 0, 0),$$

being the vertices of the unit-cube, with the omission of the corner (0, 0, 0).



For higher values of m, of course, geometrical illustration fails us.

CHAPTER IV.

TOTIENT POINTS IN THE PLANE. APPLICATIONS.

The theory of totient points in space of two dimensions is itself so extensive and furnishes such a variety of applications that we devote a separate chapter to it.

The mere fact, as indicated by the well-known equation

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} \phi_1(x)}{\frac{1}{2}x^2} = \frac{6}{\pi^2},$$

that the number of totient points in the triangle bounded by the lines $y=0$, $x=y$, $x=N$, is proportional to the area of that triangle, proves nothing as to the uniformity of distribution of such points in the plane. In this chapter we propose to prove this uniformity in the sense that if $N(k)$ is the number of points in or on the boundary of a region of area k, then

$$\lim_{k=\infty} \frac{N(k)}{K} = \frac{6}{\pi^2},$$

the area K increasing in a sense to be explained and the region to be characterized more definitely.

LEMMA. *Let $\phi_1(x, k)$ denote the number of integers less than or equal to $[k]$ and prime to x, then*

$$\phi_1(x, k) = \frac{k}{x}\phi_1(x) + \Delta_{\phi_1(x, k)},$$

where $$|\Delta_{\phi_1(x, k)}| \leqq x^{\log 2}.$$

For $k>0$ we know that

$$\phi_1(x, k) = \sum_{(d)} \mu(d)\left[\frac{k}{d}\right],$$

where the sum extends over all d's which are divisors of x. Put

$$\left[\frac{k}{d}\right] = \frac{k}{d} - \sigma_{(k, d)},$$

where $0 \leqq \sigma_{(k, d)} < 1$.

We have then $$\phi_1(x, k) = k\sum_{(d)} \frac{\mu(d)}{d} + \Delta_{\phi_1(x, k)},$$

where $\Delta\phi_1(x, k) = -\sum \sigma_{(k, d)}\mu(d)$. Suppose $x = \prod_{i=1}^{r} p_i^{a_i}$. Since now $\mu(d)=0$, when d contains a square factor, we have $\Delta_{\phi_1(x, k)} = -\sum_{(d')} \sigma_{(k, d')}\mu(d')$, where the sum now extends over all d''s which divide $x' = \prod_{i=1}^{r} p_i$. Give now σ and μ their maximum value, unity; then

$$|\Delta\phi_1(x, k)| \leqq 2^r,$$

2^r being the number of divisors of x'. Now, unless x is 1, 2 or 6, we have $x > e^r$, where e is the Naperian base, or $r \leqq \log x$. With these exceptions, therefore,

$$|\Delta\phi_1(x, k)| \leqq 2^{\log x} \leqq x^{\log 2}.$$

$$\text{Hence if } \begin{cases} x = 1, & \Delta\varphi(1, k) = 0 & < 1^{\log 2}, \\ x = 2, & \Delta\varphi(2, k) = 1 \text{ or } 0 & < 2^{\log 2}, \\ x = 6, & \Delta\varphi(6, k) = 0, 1 \text{ or } 2 & < 6^{\log 2}. \end{cases}$$

and so the lemma is completely established.

The same proof applies to totient points with negative ordinates. The lemma shows to what degree of approximation the number of totient points on any line is proportional to the length of that line.

It is important for certain applications to generalize the problem before us in that we subject the points to certain conditions. We discuss first the following problem:

PROBLEM. *To find for every real number a, and every angle $\alpha\left(0 < \alpha < \frac{\pi}{2}\right)$, the number, $N(a, \alpha)$, of pairs of integers, (x, y), which satisfy the following conditions:*

$$\begin{aligned} &[x, y] = 1, \\ &x \equiv 0 \pmod{k}, \\ &\frac{y}{x} \leq \tan\alpha, \\ &x \leq a. \end{aligned}$$

We are seeking, in fact, the number of totient points whose abscissæ are multiples of a given number k, and which lie in or on the boundary of a triangle AOB whose angle at the origin O is α, and whose side OA lies in the direction of the axis of x, the angle α being acute.

The number of totient points on any ordinate y whose abscissa is kx, is the number of integers less than or equal to y and prime to kx, which, by our lemma, is

$$y\frac{\phi_1(kx)}{kx} + \Delta_{\phi_1(kx,\, y)},$$

where $$|\Delta\phi_1(kx, y)| \leq (kx)^{\log 2}.$$

The number of points in question is then

$$N(a, \alpha) = \sum_{x=1}^{\left[\frac{a}{k}\right]} y\,\frac{\phi_1(kx)}{kx} + \Delta\phi_1(kx, y),$$

But the length of any ordinate y is $kx \tan \alpha$, so

$$N(a, \alpha) = \sum_{x=1}^{\left[\frac{a}{k}\right]} \tan \alpha \, \phi_1(kx) + \Delta\phi_1(kx, y),$$
$$= A + B,$$

where
$$A = \sum_{x=1}^{\left[\frac{a}{k}\right]} \tan \alpha \, \phi_1(kx),$$

and
$$B = \sum_{x=1}^{\left[\frac{a}{k}\right]} \Delta\phi_1(kx, y).$$

By our lemma
$$|B| \leqq \sum_{x=1}^{\left[\frac{a}{k}\right]} (kx)^{\log 2},$$
$$\leqq \sum_{x=1}^{a} x^{\log 2},$$
$$\leqq A_1 a^{\log 2 + 1},$$

where A_1 is finite and independent of a (Theorem I, Chapter II). Now the sum A is nothing less than $\Phi_1(a, 1, k) \tan \alpha$, and by Theorem VI, Chapter II, this is equal to

$$\frac{6}{\pi^2} \frac{a^2}{2} \tan \alpha \, P_{(1, k)} + \tan \alpha \, \Delta\Phi_1(a, 1, k),$$

where $|\Delta\Phi_1(a, 1, k)| \leqq A_2 a \log a$. A_2 being finite and independent of a.

Now, $\frac{a^2}{2} \tan \alpha$ is equal to the area, K, of the triangle OAB. Putting together the above results, we have

$$N(a, \alpha) = \frac{6}{\pi^2} K P_{(1, k)} + \Delta N(a, \alpha),$$

where
$$|\Delta N(a, \alpha)| \leqq A \tan \alpha \log a + B a^{\log 2 + 1},$$

A and B being finite and independent of a and α.

Take, now, another triangle OAB' having the same base $OA = a$, and a

smaller central angle α'. We see at once that the number, $N(t)$, of points (x, y) where

$$[x, y] = 1$$

and

$$x = 0 \pmod{k},$$

which lie in the triangle BOB', is given by the equation

$$N(t) = \frac{6}{\pi^2} t P_{(1, k)} + \Delta N(t),$$

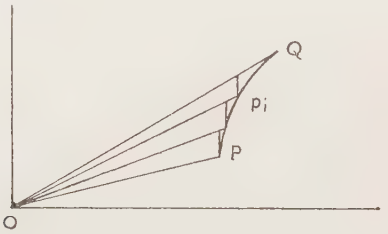
where t is the area of the triangle BOB', and

$$|\Delta N(t)| \leqq A \tan \alpha \, a \log a + B a^{\log 2 + 1},$$

A and B being independent of a and α.

Consider, now, a curve, PQ, whose polar equation is

$$r = f(\theta),$$



f being a single-valued, continuous function of θ, for

$$0 \leqq \alpha_0 \leqq \theta \leqq \alpha_1 < \frac{\pi}{2}.$$

We suppose, to avoid unimportant exceptions, that PQ is not a straight line through the origin, nor made up in part of such lines.

Join P and Q to the origin O and call the area $POQ = K$ and the angle $POQ = \beta$. Suppose, further, that the line OQ makes an angle α with Ox, where $\alpha \leqq \alpha_1$; and, for simplicity, suppose the figure OPQ to lie in the first quadrant. Divide β into n equal angles θ_n, so that $\theta_n = \frac{\beta}{n}$. Let the separating lines of these angles cut PQ in the $n = 1$ points, p_i, and through these points draw parallels to the y axis. We thus get n triangles t_j $(j = 1 \ldots . n)$.

Let $K_{(n)} = \sum_{j=1}^{n} t_j$ be the sum of the areas of these triangles. By choosing n large enough—say n_ϵ—we may make

$$\left| \frac{K - K_{n_\epsilon}}{K} \right| = \eta_{(n_\epsilon)},$$

where $\eta_{(n_\epsilon)} < \frac{\epsilon}{2}$ where ϵ is an arbitrarily small positive number taken in advance.

By what precedes, the number of points (x, y) such that $[x, y] = 1$, and $x \equiv 0 \pmod{k}$, which lie in or on the boundaries of the triangles t_j, will be

$$N(K_{n_\epsilon}) = \frac{6}{\pi^2} P_{(1,k)} K_{(n_\epsilon)} + \Delta N(K_{(n_\epsilon)}),$$

where

$$|\Delta N(K_{(n_\epsilon)})| \leqq \sum_{j=1}^{n_\epsilon - 1} A \tan\alpha \, a_j \log a_j + B a_j^{\log 2 + 1},$$

where a_j is the abscissa of p_j. Let R be the largest of these abscissæ, then

$$|\Delta N(K_{n_\epsilon})| \leqq (n_\epsilon - 1)\{A \tan\alpha \, R \log R + BR^{\log 2+1}\},$$
$$\leqq \frac{\beta}{\theta_{n_\epsilon}}\{A \tan\alpha \, R \log R + BR^{\log 2+1}\}.$$

Now we have
$$K_{n_\epsilon} = K - (K - K_{n_\epsilon}),$$
$$= K - K\eta_{(n_\epsilon)}.$$

Also
$$N(K_{n_\epsilon}) = N(K) - N(K - K_{n_\epsilon}),$$

and since
$$N(K - K_{n_\epsilon}) < K - K_{n_\epsilon} < \eta_{(n_\epsilon)} K,$$

we have
$$N(K) = \frac{6}{\pi^2} K P_{(1,k)} + \Delta N(K),$$

where

$$|\Delta N(K)| \leqq \frac{\beta}{\theta_{n_\epsilon}} \{A \tan\alpha \, R \log R + BR^{\log 2+1}\} + CK\eta_{(n_\epsilon)},$$

where, further,
$$|C| \leqq 1 + \frac{6}{\pi^2} P_{(1,k)} < 2.$$

We have then

$$\left| \frac{\Delta N(K)}{K} \right| \leqq \frac{\beta}{\theta_{(n_\epsilon)}} \left\{ \frac{A \tan\alpha \, R \log R}{K} + \frac{BR^{\log 2+1}}{K} \right\} + 2\eta_{(n_\epsilon)}.$$

Multiply, now, every ordinate and every abscissa by M. This multiplies R by M and K by M^2. It leaves β, α, $\theta_{(n_\epsilon)}$ and $\eta_{(n_\epsilon)}$ unchanged. Calling the new area $\overline{K}$, we have

$$\left|\frac{\Delta N(\overline{K})}{\overline{K}}\right| \leq \frac{\beta}{\theta_{(n\epsilon)}}\left\{\frac{A\tan\alpha\, R\log RM}{MR} + \frac{BR^{\log 2+1}}{M^{1-\log 2}K}\right\} + 2\eta_{(n_\epsilon)}.$$

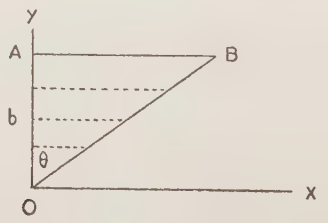
By making M arbitrarily large, we may make this ratio approach as nearly as we please to the quantity $2\eta_{(n_\epsilon)}$, which is less than the arbitrarily small quantity ϵ. The ratio $\frac{N(K)}{K}$ approaches, therefore, the limit $\frac{6}{\pi^2}P_{(1,k)}$, as the area K is increased in the above manner. It is now seen why we restricted α to be less than $\frac{\pi}{2}$. Since totient points are symmetric with respect to the axis of x, the curve may cross the x axis. By horizontal summation we can establish the same result for curves crossing the y axis as follows:

Writing $x = mk$, we see that for a totient point it is necessary that $[m, y] = 1$.

1st. Suppose $[k, y] = 1$. On any abscissa of length equal to x, there will be as many totient points as there are values of m such that $[m, y] = 1$, and $m \leq \frac{x}{k}$, which number, as we know, is $\frac{x}{k}\frac{\phi_1(y)}{y} + \Delta\phi_1\left(\frac{x}{k}, y\right)$, where $\left|\Delta\phi_1\left(\frac{x}{k}, y\right)\right| \leq y^{\log 2}$.

2nd. Suppose $[k, y] \neq 1$; then, instead of the above result, we should count none at all, since on such an abscissa $[x, y] \neq 1$. Our plan is naturally to effect the sum for all abscissæ under the first supposition, and then correct for those where $[k, y] \neq 1$.

Take our triangle now as in the figure, with base b on the y axis, and let



the angle $AOB = \theta$. Then $x = y \tan\theta$. Under the first supposition the sum is

$$\sum_{y=1}^{[b]} \frac{x}{k} \frac{\phi_1(y)}{y} + \sum_{y=1}^{[b]} \Delta\phi_1\left(\frac{x}{k}, y\right).$$

For the abscissæ where y is a multiple of p_i, one of the factors of k, we have to reject

$$\sum_{y=1}^{\left[\frac{b}{p_i}\right]} \frac{x}{k} \frac{\phi_1(p_i y)}{p_i y} + \sum_{y=1}^{\left[\frac{b}{p_i}\right]} \Delta\phi_1\left(\frac{x}{k}, p_i y\right).$$

By applying the principle of cross-classification, the result is easily seen to be

$$N(t) = \sum_{y=1}^{\left[\frac{b}{d}\right]} \sum_{(d)} \frac{x}{k} \mu(d) \frac{\phi_1(yd)}{yd} + \Delta\phi_1\left(\frac{x}{k}, yd\right),$$

where the inner sum runs over all d's which are divisors of k. For each value dy of the argument, $x = dy \tan\theta$, so the result may be written, changing the order of summation,

$$N(t) = \frac{\tan\theta}{k} \sum \mu(d) \sum_{y=1}^{\left[\frac{b}{d}\right]} \phi_1(yd) + \sum_{y=1}^{\left[\frac{b}{d}\right]} \sum_{(d)} \Delta\phi_1\left(\frac{x}{k}, yd\right),$$

or, in our usual notation,

$$N(t) = \frac{\tan\theta}{k} \sum_{(d)} \mu(d) \Phi_1(b, 1, d) + \sum_{y=1}^{\left[\frac{b}{d}\right]} \sum_{(d)} \Delta\phi_1\left(\frac{x}{k}, yd\right).$$

We then have

$$N(t) = \frac{\tan\theta}{k} \frac{6}{\pi^2} \frac{b^2}{2} \sum_{(d)} \mu(d) P_{(1, d)} + \Delta N(t);$$

where $$|\Delta N(t)| \leqq A \tan\theta\, b \log b + B b^{\log 2 + 1}.$$

Now, it is easily seen that

$$\sum_{(d)} \mu(d) P_{(1, d)} = \prod_{i=1}^{r} (1 - P_{(1, p_i)}),$$

where the product extends over all the primes p_i which divide k. But since

$P_{(1,\,p_i)} = \dfrac{1}{p_i+1}$, the above product may be written

$$\prod_{i=1}^{r} \frac{p_i}{p_i+1},$$

which, when divided by k, is precisely $P_{(1,\,k)}$, and since further $\dfrac{b^2}{2}\tan\theta = K$, the area of the triangle, we have

$$N(t) = \frac{6}{\pi^2} P_{(1,\,k)} K + \Delta N(t),$$

the limits of Δ being as above. The rest of the argument now proceeds as before. We see incidentally that we would have obtained the same result in the first instance if we had used the condition $y \equiv 0 \pmod{k}$, instead of $x \equiv 0 \pmod{k}$. A finite number of additions and subtractions will not alter the degree of the residue function, and we now may state the theorem:

THEOREM I. *Given a closed contour decomposable into a finite* number of segments of the type considered. Let the area of the region bounded by this contour be K, and let $N(K, \mid k)$ be the number of points (x, y) in or on the boundary such that*

$$[xy] = 1,$$
$$x \equiv 0 \pmod{k},$$

then

$$\lim_{k=\infty} \frac{N(K, \mid k)}{K} = \frac{6}{\pi^2} P_{(1,\,k)},$$

where K increases by ordinary magnification, all the lines of the figure being lengthened proportionally, and where for $k = \prod_{i=1}^{r} p_i^{a_i}$,

$$P_{(1,\,k)} = \frac{1}{k} \prod_{i=1}^{r} \frac{p_i}{p_i+1}, \text{ but } P_{(1,\,1)} = 1.$$

The condition, $x \equiv 0 \pmod{k}$, may, as we have seen, be replaced by the conditions $y \equiv 0 \pmod{k}$, the limit remaining as before. Also, the second part of the above discussion shows that if we assume $x \equiv 0 \pmod{k}$ and $y \equiv 0 \pmod{k'}$—

* The theorem might be applied also to curves where a finite decomposition is impossible, provided the total area is a definite thing and the infinite series of residue errors suitably convergent.

where necessarily $[k, k'] = 1$—the result would have been

$$\lim_{k=\infty} \frac{N(K)}{R} = \frac{6}{\pi^2} P_{(1, k)} P_{(1, k')},$$

which may be written $\frac{6}{\pi^2} P_{(1, kk')}$.

It is further possible to impose the conditions $[x, z] = 1$, $[y, z'] = 1$, so that our point (x, y) now shall satisfy the five conditions

$$\begin{aligned} &\text{I.} && [x, y] = 1, \\ &\text{II.} && x \equiv 0 \pmod{k}, \\ &\text{III.} && y \equiv 0 \pmod{k'}, \\ &\text{IV.} && [x, z] = 1, \\ &\text{V.} && [y, z'] = 1, \end{aligned}$$

where necessarily for totient points to exist,

$$\begin{aligned} [x, k'] &= 1, \\ [k, z] &= 1, \\ [k', z'] &= 1, \end{aligned}$$

but where z and z' may or may not be relative primes.

The number of points satisfying I, II and III is, as we have just seen, $\frac{6}{\pi^2} KP_{(1, kk')}$, which, for shortness, we denote by M. Suppose, now, that $z = \prod_{i=1}^{\rho} r_i^{\alpha_i}$ and $z' = \prod_{i=1}^{\sigma} s_i^{\beta_i}$, where r_i and s_j are not necessarily distinct. We reject first those values of x which are multiples of the primes r_i. By applying the principle of cross-classification, the remaining number of points is $M \prod_{i=1}^{\rho} (1 - P(1, r_i))$, which equals $M \prod_{i=1}^{\rho} \frac{r_i}{r_i + 1}$, which equals $Mz P_{(1, z)}$. If now we suppose $[z, z'] = 1$, we reject in the same way those points where y is a multiple of s_i, and get $MzP_{(1, z)} \cdot z' \cdot P_{(1, z')}$, which is the desired result when $[z, z'] = 1$. Suppose, however, in addition that x and y are both to be prime to z''. Rejecting those values of x which are multiples of the primes of z'', we have the above result multiplied by $z'' P_{(1, z'')}$. From this we need reject now only

those points where y is also a multiple of the primes of z''. This multiplies the result again by $\phi_1(z'')$. We may put all these results in the following theorem:

THEOREM II. *Given a closed contour decomposable into a finite number of segments such that for each segment the radius vector is a single-valued, continuous function of the amplitude. Let the area of the region bounded by this contour be K, and let $N(K|, k, k', z, z', z'')$ be the number of points (x, y) such that*

$$\begin{aligned} &\text{I.} && [x, y] = 1, \\ &\text{II.} && x \equiv 0 \pmod{k}, \\ &\text{III.} && y \equiv 0 \pmod{k'}, \\ &\text{IV.} && [x, z] = 1, \\ &\text{V.} && [y, z'] = 1, \\ &\text{VI.} && [xy, z''] = 1, \end{aligned}$$

where also

$$\begin{aligned} &\text{VII.} && [k, k'] = 1, \\ &\text{VIII.} && [k, z] = 1, \\ &\text{IX.} && [k', z'] = 1, \\ &\text{X.} && [z, z'] = 1, \end{aligned}$$

$$\text{then } \lim_{K=\infty} \frac{N(K|, k, k', z, z', z'')}{K} = \frac{6}{\pi^2} zz' \phi_1(z'') P_{(1, kk')} P_{(1, zz')} P_{(1, zz'')},$$

where K increases, by ordinary magnification, all the lines of the figure being lengthened in the same proportion, and where, for $k = \prod_{i=1}^{r} p_i^{a_i}$,

$$P_{(1, k)} = \frac{1}{k} \prod_{i=1}^{r} \frac{p_i}{p_i + 1}, \text{ but } P_{(1, 1)} = 1.$$

It is not difficult to show that the restriction $ax \not\equiv by \pmod{k}$ introduces a factor $kP_{(1, k)}$.

We have seen that in space of any number of dimensions the effect of a linear transformation of determinant positive or negative unity, with positive or negative integer coefficients, is to throw totient points into totient points. We know, further, that in the plane such a transformation leaves areas unaltered. Let such a transformation be

$$\begin{aligned} x' &= \alpha x + \beta y; \\ y' &= \gamma x + \delta y; \end{aligned}$$

where $\alpha\delta - \beta\gamma = 1$. The ten conditions of the preceding theorem are now, dropping accents,

I. $[x, y] = 1$,
II. $\delta x \equiv \beta y \pmod{k}$,
III. $\gamma x \equiv \alpha y \pmod{k'}$,
IV. $[\delta x - \beta y, z] = 1$,
V. $[\gamma x - \alpha y, z'] = 1$,
VI. $[(\delta x - \beta y)(\gamma x - \alpha y), z''] = 1$.

The remaining conditions are not changed. The formula for $\lim_{k=\infty} \frac{N(K|, k, k', z, z', z'')}{K}$ is not disturbed.

We are now prepared to write out an indefinite number of theorems which are merely applications of the preceding theorems. It has been noticed (cf. Sylvester, Philosophical Magazine, 1883, p. 251), that the number of proper fractions in their lowest terms whose denominators are less than or equal to n, is approximately $\frac{3}{\pi^2} n^2$. This follows easily when thrown into the language of our theorems. We are, as a matter of fact, finding the number of pairs of integers, $[x, y]$, such that $[x, y] = 1$, and also such that $1 \leqq y \leqq x \leqq n$. Here we have the area $K = \frac{n^2}{2}$ and the number is, therefore, $\frac{6}{\pi^2} \frac{n^2}{2}$ or $\frac{3}{\pi^2} n^2$. More generally we might ask for the number of such fractions, where the numerators lie between l and $l + m$, while the denominators lie between l' and $l' + m'$. The area K is here mm', and the number in question is $\frac{6mm'}{\pi^2}$. Manifestly, the number of such theorems may be multiplied indefinitely, the one difficulty in any case being the determination of the area K which stands for the conditions of inequality.

Another class of theorems has to do with integral right triangles. By an integral right triangle we mean a right triangle whose three sides may be represented by integers. Such a triangle is said to be reduced if the three numbers which represent the sides have no common divisor except unity. It is well known* that the three sides of such a triangle are given by the formulæ

---

* See Frenicle, "Traité des triangles rectangles en nombres," Paris, 1676, §§ xxiv, xxv, pp. 59, 61; Euler, "Commentationes arithmeticæ, vol. I, pp. 24, 25. Also Annals of Mathematics, vol. I, 2d series, No. 3, p. 1.

$$a = m^2 + n^2,$$
$$b = m^2 - n^2,$$
$$c = 2mn.$$

If the triangle is to be reduced, it is further necessary and sufficient that $[m, n] = 1$, and $m \not\equiv n \pmod 2$. If we take the further condition that the hypotenuse a shall be less than or equal to N, we have $m^2 + n^2 \leq N$. If the sides are to be positive, we take $m > n$. We may take m and n both positive, since $-m$ and $-n$ give the same triangles as $+m$ and $+n$. These conditions give an area K equal to $\frac{N\pi}{8}$. Our number, therefore, is $\frac{6}{\pi^2}\ \frac{N\pi}{8}\ 2P_{(1,2)}$ or $\frac{N}{2\pi}$. Thus for $N = 100$, $\frac{N}{2\pi} = 15.9$, and actual count gives 16 triangles.

If, instead of restricting the hypotenuse as above, we restrict the sum of the three sides to be less than or equal to N, we easily get the formula $\frac{N}{\pi^2}\log 2$. Manifestly, here also the number of special problems may be indefinitely extended.

The foregoing problem is of special importance in that it suggests a class of theorems of which it is a very special case. For any number to serve as the largest side of such a triangle, it is necessary and sufficient that it should be expressible as the sum of two squares which are relative primes. But the necessary and sufficient condition that it be so expressible is that every one of its prime divisors be of the form $4n + 1$. Further, if the order of the squares be left out of account, a number x of this sort can be so expressed in $2^{\nu(x)-1}$ different ways, where $\nu(x)$ is the number of distinct prime divisors of x. We have, then, the theorem

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)}\, \Theta_{(4,1)}(x)}{N} = \frac{1}{\pi}.$$

where the function $\Theta_{(4,1)}(x)$ is equal to 1 or 0, according as all the prime factors of x are or are not of the form of $4n + 1$. This is, then, a particular case of the theorem noted in the Introduction.

We now proceed to consider representations of numbers by the binary quadratic form

$$ax^2 + 2bxy + cy^2,$$

where $[a, 2b, c] = 1$, these representations to conform to the three conditions

$$\text{I.} \quad [x, y] = 1,$$
$$\text{II.} \quad 0 < ax^2 + 2bxy + cy^2 \leqq N,$$
$$\text{III.} \quad [ax^2 + 2bxy + cy^2, 2D] = 1,$$

where $D = b^2 - ac$.

We may suppose $[a, 2D] = 1$ (Dirichlet-Dedekind "Zahlentheorie," p. 233), and, therefore, $[a, b] = 1$. Now we have

$$a(ax^2 + 2bxy + cy^2) = (ax + by)^2 - Dy^2.$$

We may, therefore, replace condition III by

$$[ax + by, 2D] = 1.$$

Our result is, therefore, $\frac{6}{\pi^2} K 2D P_{(1, 2D)}$. The area K is to be determined from the second condition, and is very different in form according as D is positive or negative; that is, for Definite or Indefinite forms.

For Definite forms, where D is negative and equal to $-\Delta$, the area is bounded by the ellipse

$$ax^2 + 2bxy + cy^2 = N.$$

We have, then, $K = \frac{\pi N}{\sqrt{\Delta}}$, and the number of points in this case satisfying the given conditions is

$$\frac{12}{\pi} N \sqrt{\Delta} P_{(1, 2\Delta)}.$$

For Indefinite forms, we may have an infinite number of representations of a number m by one and the same form. Thus, if

$$ax^2 + 2bxy + cy^2 = m$$

be a representation of m, so also is

$$a\xi^2 + 2b\xi\eta + c\eta^2 = m,$$

where

$$\xi = U_{(n)}.(bx + cy) \pm T_{(n)}.x,$$
$$\eta = U_{(n)}(ax + by) \mp T_{(n)}.y,$$

where $(T_{(n)}, U_{(n)})$ is any one of the infinite number of solutions of

$$t^2 - Du^2 = 1.$$

Now, it is well known (Dirichlet-Dedekind "Zahlentheorie," p. 247) that one of these solutions may be isolated from the rest by the conditions

$$y > 0,$$
$$U(ax + by) - Ty > 0.$$

These conditions define a hyperbolic sector within which all our points must lie, which is bounded by the lines

$$ax^2 + 2bxy + cy^2 = N,$$
$$y = 0,$$
$$U(ax + by) - Ty = 0,$$

the area of which is

$$\frac{N}{2\sqrt{D}} \log (T + U\sqrt{D}),$$

(T, U) being the fundamental or smallest solution of the Pellian equation $t^2 - Du^2 = 1$. This being our area K, our number of points in this instance is

$$\frac{6}{\pi^2} \sqrt{D}\, P_{(1, 2D)}\, N \log (T + U\sqrt{D}).$$

If we multiply the above results by h, the number of properly primitive classes of determinant D, we get the total number of properly primitive representations of numbers less than or equal to N and prime to $2D$. This number is otherwise expressible as follows: Let x be any number prime to $2D$, and let $\nu(x)$ be the number of its distinct prime factors. If D is not a quadratic residue of each one of these prime factors, x is not capable of primitive representation by any form of determinant D. If, however, D is a quadratic residue of every prime factor of x, then the number of primitive representations of x by properly primitive forms of determinant D is $\varepsilon 2^{\nu(x)}$, where ε is the number of solutions of the Pellian equation $t^2 - Du^2 = 1$.

In the case of Definite forms $\varepsilon = 2$, except for the single case $D = -1$, where $\varepsilon = 4$.

In the case of Indefinite forms, the number of solutions of the Pellian equation is infinite, but our isolating conditions noted above amount to making $\varepsilon = 1$.

Now the primes, of which D is a quadratic residue, belong to a certain set s of linear forms (Dirichlet-Dedekind, "Zahlentheorie," p. 121). If x is then made up of primes belonging to these forms, we get $2^{\nu(x)}$ primitive representations,

otherwise none at all. If, then, as in the Introduction, we define a function $\Theta_s(x)$, which equals 1 or 0, according as each prime divisor of x does or does not belong to a form of the set s of linear forms, we may write for the above number of properly primitive representations

$$\varepsilon \sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x).$$

For Definite forms this gives

$$\varepsilon \lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \frac{12}{\pi} h\sqrt{\Delta}\, P_{(1,\,2\Delta)}.$$

For Indefinite forms, we get

$$\varepsilon \lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \frac{6}{\pi^2} h\sqrt{D}\, P_{(1,\,2D)} \log(T + U\sqrt{D}).$$

We have thus established, for a large number of cases, the theorem mentioned in the Introduction. The method will not avail to establish the law for other systems of forms s, such as for example the single form $4n - 1$, where the law seems to be

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \frac{2}{\pi}.$$

The form $4n - 1$ belongs to quadratic forms only in connection with other linear forms.

From these last equations we may derive new expressions for the number h of properly primitive classes of determinant D.

For Definite forms

$$h = \varepsilon \frac{\pi}{12} \cdot \frac{1}{\sqrt{\Delta}}\, P_{(1,\,2\Delta)} \lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N}.$$

For Indefinite forms,

$$h = \frac{\pi^2}{6\sqrt{D}} \cdot \frac{1}{P_{(1,\,2D)} \log(T + U\sqrt{D})} \lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N}.$$

Again, from the well-known formulæ for h (Dirichlet-Dedekind, "Zahlentheorie," §§97–101), we may write the equation for Definite forms,

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \frac{12}{\pi^2} \Delta P_{(1,\, 2\Delta)} \sum_{i=1}^{\infty} \frac{1}{i} \left(\frac{D}{i}\right).$$

where, on the right, the sum (which is not independent of the order of the terms) is arranged according to increasing values of i, the symbol $\left(\frac{D}{i}\right)$ being Jacobi's symbol.

For Indefinite forms, the equation is

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_s(x)}{N} = \frac{12}{\pi^2} DP_{(1,\, 2D)} \sum_{i=1}^{\infty} \frac{1}{i} \left(\frac{D}{i}\right).$$

From these last two expressions, we observe that if s and s' denote the sets of linear forms belonging to binary quadratic forms of determinants D and $-D$ respectively, we have

$$\lim_{N=\infty} \frac{\sum_{i=1}^{N} 2^{\nu(x)} \Theta_s(x)}{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_{s'}(x)} = \frac{\sum_{i=1}^{\infty} \frac{1}{i} \left(\frac{-D}{i}\right)}{\sum_{i=1}^{\infty} \frac{1}{i} \left(\frac{D}{i}\right)}.$$

Let us restrict ourselves to numbers m_i, which belong to a particular form of the above set s of linear forms. (Clearly the factors of m_i may or may not belong to this particular form.) This restriction might be written as a congruential condition on m_i. It might then be written as a congruential condition on x and y. The modulus of this congruential relation would depend only on the modulus of the forms of the system s, and so would be the same, whatever particular form we have selected. Each linear form of s, therefore, furnishes the same number to the above sum, and the number thus furnished by each is the total number divided by the number of forms in s.

Now, the total number of linear forms belonging to a quadratic form of determinant D is well known. (Cf. H. J. S. Smith, Works, vol. I, pp. 206, 207.) If we write

$$D = 2^{\alpha} \prod_{i=1}^{r} p_i^{a},$$

where the p_i's are odd primes, the number in question is

$$\tfrac{1}{2}\phi_1(2^k D'),$$

where $D' = \prod_{i=1}^{r} p_i$ and k is given as follows:

$$k = 1, \text{ when } D \equiv 1 \text{ or } 5 \pmod 8,$$
$$k = 2, \quad " \quad D \equiv 3, 4 \text{ or } 7 \pmod 8,$$
$$k = 3, \quad " \quad D \equiv 0, 2 \text{ or } 6 \pmod 8.$$

But $\frac{1}{2}\phi_1(2^k D') = 2^{k-2}\prod_{i=1}^{r}(p_i - 1)$, so that we have for each form

$$\frac{12}{\pi}\ \frac{D}{2^{k-2}}\ \frac{P_{(1,\,2D)}}{\prod_{i=1}^{r}(p_i - 1)}\ K.$$

This is not a case of the theorem noted in the Introduction. In this we have imposed the further restriction that the number x should belong itself to a particular form, its factors belonging to the forms of s.

CHAPTER V.

Further Results and Desiderata.

The theory of totient points in space of m dimensions is as yet incomplete. Proofs of the following theorems have been obtained, however:

THEOREM I. *Denoting by* $\phi_m(x, k_1, k_2, \ldots, k_m)$ *the number of sets of integers* $x_1 x_2 \ldots x_m$ *such that* $[x, x_1, x_2, \ldots, x_m] = 1$ *and* $x \geqq k_i \geqq x_i \geqq 1$, *we have*

$$\phi_m(x, k_1, \ldots k_m) = \sum_{(d)} \prod_{i=1}^{m} \left[\frac{k}{d}\right] \mu(d),$$

the sum extending over all d's which are divisors of x.

By means of this we get

THEOREM II. $\phi_m(x, k_1, \ldots, k_m) = \prod_{i=1}^{m} k_i \frac{\phi_m(x)}{x^m} + \Delta\phi_m(x, k_1, \ldots, k_m)$, *where* $|\Delta\phi_m(x, k_1, \ldots, k_m)| \leqq A\bar{k}^{m-1} x^{\log 2}$, *where* A *is finite and independent of* x, *and* $\bar{k}$ *is the largest of the parameters* k_i.

This theorem is seen to be a generalization of the lemma of Chapter IV. By means of it we have established a certain "density theorem" for totient points in space of m dimensions. We use the following notions and definitions:

An m dimensional surface is the locus of points $(x_1, x_2, \ldots, x_m)$ satisfying a single relation $F(x_1, x_2, \ldots, x_m) = 0$. Two points not on the surface will be said to lie on *opposite sides* if, when their coordinates are substituted in $F(x_1, x_2, \ldots x_m)$, the two results are different in sign.

If all the points lying on one side of a surface have all their coordinates finite, the surface will be called *closed*, and the points will be said to be on the *inside*.

The *content* of a closed surface will be defined by the integral

$$V_{(m)} = \int_{x_1} \int_{x_2} \cdots \int_{x_m} dx_1\, dx_2 \ldots dx_m,$$

the limits being taken so as to include all the elements $dx_1 dx_2 \ldots dx_m$ lying on the inside of the surface.

We speak also of the *intersection* of two m dimensional surfaces as the locus of points satisfying the equations of both. Points lying on a definite side of each surface may have all their coordinates finite, in which case we may speak of the content enclosed by the two surfaces.

We have then established the following theorem:

THEOREM III. *The number of totient points within or on any closed surface of m dimensions being denoted by $N(V)$, where V is the content of the surface, we have*

$$\lim_{V=\infty} \frac{N(V)}{V} = \frac{1}{\sum_{i=1}^{\infty} \frac{1}{i^m}},$$

where the content V is supposed to increase by multiplying the coordinates of every point on the surface by the same multiplier.

We have not discussed those cases where the coordinates are subjected to further restrictions. It is hoped that theorems concerning primitive representation by m-ary forms may be obtained, with perhaps applications similar to those obtained in the case of binary quadratic forms.

A method of discussing the following problem is also still lacking:

"To prove or disprove the equation

$$\lim_{N=\infty} \frac{\sum_{x=1}^{N} 2^{\nu(x)} \Theta_{(a,\,b)}(x)}{x} = \text{constant},$$

where $\Theta_{(a,\,b)}(x) = 1$ or 0, according as all the $\nu(x)$ distinct primes in x are or are not of the form $an + b$ where $[a, b] = 1$."

A proof of this theorem, if it is true, would furnish easily a proof of Dirichlet's theorem that the number of primes of the form $an + b$, where $[a, b] = 1$ is infinite. We have, as we have seen, proved the theorem for the forms $4n + 1$ and $6n + 1$, which belong to the forms $x^2 + y^2$ and $x^2 + 3y^2$ respectively. For quadratic forms in general, we have to reckon with more than one linear form.

In connection with this last theorem, we have established the following equation, which may be of assistance in solving the problem:

$$\sum_{x=1}^{[N]} 2^{\nu(x)}\,\Theta_{(a,\,b)}(x) = \sum_{x=1}^{[N]} T\left(\frac{N}{x}\right)\mu(x),$$

where $T(k) = \sum_{j=1}^{[k]} \prod_{i=1}^{r}{}_{(j)} (1 + 2\alpha_i)$, where also $j = \prod_{i=1}^{r} p_i^{\alpha_i} \prod_{i=1}^{s} q_i^{\beta_i}$, where, we suppose, p_i and q_i are primes ≥ 1 such that

$$p_i = an + b,$$
$$q_i \neq an + b.$$

VITA.

I, Derrick Norman Lehmer, was born July 27, 1868, in Somerset, Wabash county, Indiana. I received my early training in the public schools of Nebraska. I entered the Preparatory Department of the University of Nebraska in 1887, and was graduated in that institution in 1893, taking the degree of B. A. I studied one year at Johns Hopkins University ('93–'94) where I heard lectures by Professors Craig, Franklin, and Study. After a year of civil engineering I returned to the University of Nebraska as Fellow in Mathematics, where I studied with Professor Davis. I took the degree of M. A. in '96 at that institution. In '98 I was appointed to a Fellowship in Mathematics at the University of Chicago, where I have had work with Professors Moore, Bolza and Maschke.